СОГЛАСОВАНО
И.о. министра цифрового развития и связи
Новосибирской области

_____ И.О. Савельева
М.П.
«24» 06 2025 г.

УТВЕРЖДАЮ
Министр труда и социального развития
Новосибирской области

_____ Е.В. Бахарева
М.П.
«24» 06 2025 г.

РЕГЛАМЕНТ ПОДКЛЮЧЕНИЯ

к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области»

СОГЛАСОВАНО
Руководитель государственного
бюджетного учреждения Новосибирской
области «Центр защиты информации
Новосибирской области»

_____ Д.А. Домшинский

2025

Содержание

Перечень принятых сокращений

АРМ	–	автоматизированное рабочее место
ИС	–	информационная система
МЭ	–	межсетевой экран
НСД		несанкционированный доступ
ПАК	–	программно-аппаратный комплекс
ПК	–	программный комплекс
САВЗ	–	средство антивирусной защиты
САНЗ	–	средство анализа защищенности
СЗИ	–	средство защиты информации
СКЗИ	–	средство криптографической защиты информации
СОВ	–	средство обнаружения вторжений
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю

1. Основные положения

Настоящий Регламент подключения к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (далее – Регламент) определяет состав участников информационного взаимодействия, порядок подключения и технические условия при подключении к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (далее – ТИС СПГ, информационная система).

Настоящий Регламент распространяется на всех участников информационного взаимодействия, которым необходимо подключение к информационным ресурсам ТИС СПГ (далее – организации-заявители).

Для подключения к ТИС СПГ (серверному сегменту) требуется обеспечить подключение к защищенной ViPNet-сети № 985 и выполнить требования по защите информации, определенные оператором ТИС СПГ – министерством труда и социального развития Новосибирской области совместно с министерством цифрового развития и связи Новосибирской области.

2. Общие сведения об информационной системе

Назначением ТИС СПГ является:

- обеспечение процессов осуществления министерством труда и социального развития Новосибирской области и подведомственными ему государственными учреждениями, учреждениями социального обслуживания населения в муниципальных образованиях Новосибирской области, отделами организации социального обслуживания населения администраций муниципальных образований Новосибирской области, отделами опеки и попечительства администраций муниципальных образований Новосибирской области функций и предоставления услуг в сфере социальной защиты населения;
- автоматизации процессов предоставления мер социальной защиты (поддержки), социальных услуг в рамках социального обслуживания и государственной социальной помощи, предоставляемых гражданам в Новосибирской области.

ТИС СПГ предназначен для решения задач:

- обеспечение предоставления государственных услуг министерства труда и социального развития Новосибирской области отдельным категориям граждан;
- обеспечение ведения областного регистра отдельных категорий граждан, проживающих на территории Новосибирской области, имеющих право на меры социальной поддержки;
- повышение адресности и качества предоставления социальных услуг и оказания социального обслуживания;
- достижение необходимого уровня вариативных форм и видов социальной поддержки для нуждающихся граждан;
- учет граждан, признанных нуждающимися в социальном обслуживании - получателей государственных услуг;
- осуществление информационного обмена в рамках имеющихся соглашений;
- формирование отчетности о предоставлении гражданам мер социальной поддержки и социальных выплат.

ТИС СПГ создана и функционирует в соответствии с постановлением Правительства Новосибирской области от 30.12.2015 № 483-п «О создании государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области».

Для ТИС СПГ установлен **второй уровень защищенности персональных данных** (УЗ-2) (далее – ПДн) в соответствии с Требованиями к защите персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 01.11.2012 № 1119.

Для ТИС СПГ установлен **второй класс защищенности** (К2) в соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденным приказом ФСТЭК России от 11.02.2013 № 17.

3. Общие требования по защите информации

В соответствии с нормативными правовыми актами в области защиты информации в ТИС СПГ и во внешних информационных системах организаций-заявителей, подключаемых к ТИС СПГ, (далее – внешние ИС) должны быть приняты меры по защите содержащейся в них информации.

Подключение внешних ИС к ТИС СПГ должно осуществляться в соответствии с:

– требованиями нормативных правовых актов РФ в области защиты информации в соответствии с Приложением № 1;

– требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти РФ в области обеспечения безопасности информации (ФСТЭК России, ФСБ России);

– настоящим Регламентом.

Для организации защищенного взаимодействия внешних ИС с информационными ресурсами ТИС СПГ во внешней ИС должны быть выполнены организационные и технические мероприятия, подтверждающие соответствие системы защиты информации внешней ИС требованиям безопасности информации.

Для выполнения требований по защите информации при работе с ресурсами ТИС СПГ, во внешней ИС требуется обеспечение второго класса защищенности (К2) ИС и второго уровня защищенности ПДн (УЗ-2).

Ответственность за организацию работ и выполнение мероприятий по защите информации при подготовке к подключению и эксплуатации внешней ИС возлагается на руководителя организации-заявителя. Обеспечение защиты информации в ходе эксплуатации внешней ИС осуществляется ее владельцем в соответствии с организационно-технической, организационно-распорядительной, эксплуатационной документацией на систему защиты информации внешней ИС и нормативно-техническими документами РФ в области защиты информации.

В соответствии с Федеральным законом от 27.06.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», а также приказом ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» обеспечение безопасности персональных данных достигается в частности:

– применением сертифицированных ФСТЭК России средств защиты информации;

– оценкой эффективности принимаемых мер по защите информации до ввода в эксплуатацию информационной системы;

– контролем за принимаемыми мерами по защите информации;

– проведение аттестационных испытаний внешней ИС на соответствие требованиям защиты информации не ниже третьего класса защищенности.

В случае привлечения организации для проведения работ по защите информации в ходе создания, эксплуатации и оценки эффективности внешней ИС в соответствии с законодательством РФ, данная организация должны иметь:

– лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, проектирования в защищенном исполнении средств и систем информатизации, установки и монтажа средств защиты информации;

– лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

Выбор организации-лицензиата осуществляется организацией-заявителем самостоятельно.

4. Порядок подключения

4.1. Требования по защите информации

Для обеспечения выполнения требований по защите информации во внешних ИС должны применяться средства защиты информации, имеющие действующие сертификаты соответствия требованиям безопасности информации ФСТЭК России и ФСБ России.

Во внешних ИС второго класса защищенности должны применяться:

– средства вычислительной техники не ниже 5 класса;
– средства защиты информации не ниже 5 класса;
– средства защиты информации, соответствующие 5 или более высокому уровню доверия.

Функции безопасности средств защиты информации должны обеспечивать выполнение мер по защите информации.

Для организации защищенного канала связи между ТИС СПГ и внешней ИС необходимо применение сертифицированных средств криптографической защиты информации, совместимых со средствами криптографической защиты информации, применяемыми в защищенной сети Правительства Новосибирской области и построенными на основе технологии виртуальных частных сетей (VPN) путем применения криптографических методов, построенному с использованием средств продуктовой линейки ViPNet Network Security класса КС1 и выше для второго класса защищенности (К2) ИС. Средство криптографической защиты информации может быть как программным, так и программно-аппаратным.

Для реализации мер защиты информации во внешней ИС должны применяться следующие средства защиты информации:

– средство защиты информации от несанкционированного доступа и/или сертифицированная ФСТЭК России ОС (СЗИ от НСД);
– средство антивирусной защиты (САВЗ);
– средство обнаружения вторжений (СОВ);
– средство анализа защищенности (САНЗ);
– межсетевой экран (МЭ);
– средство защиты виртуальной инфраструктуры (СЗИ ВИ);

– средство криптографической защиты информации (СКЗИ);
– машинный носитель аутентификационной информации (Токен).

Пример средств защиты информации, необходимых к применению во внешних ИС, представлен в таблице 2 Приложения № 2.

В случае несоответствия имеющихся средств защиты или отсутствия необходимых средств защиты, организация-заявитель проводит закупку дополнительного программного обеспечения для установки на АРМ, включенные во внешнюю ИС.

Согласно пояснительной записке к техническому проекту на систему защиты информации, обрабатываемой в государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области», для обеспечения безопасности в информационных системах, подключаемых к ТИС СПГ, должен быть реализован набор мер защиты информации, указанный в таблице 1 Приложения № 2.

4.2. Обеспечение требований к организационным мерам защиты информации внешней ИС

Организационные меры защиты включают:

– определение класса защищенности внешней ИС и уровня защищенности обрабатываемых в ней персональных данных с составлением соответствующих актов;

– определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации при ее обработке во внешней ИС (разработка Модели угроз и нарушителя безопасности информации);

– определение требований к системе защиты информации во внешней ИС (разработка Технического задания на систему защиты информации);

– проектирование системы защиты информации, определяющее и описывающее реализуемые меры по защите информации согласно Техническому заданию;

– организацию контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования внешней ИС;

– контроль физического доступа к программно-аппаратным средствам, коммутационному и телекоммуникационному оборудованию и линиям связи внешней ИС;

– организацию учета и хранения машинных носителей информации во внешней ИС;

– назначение должностного лица, ответственного за организацию обработки и обеспечение безопасности ПДн при их обработке во внешней ИС;

– определение перечня пользователей, имеющих доступ к внешней ИС и прав, необходимых пользователю для работы в ИС;

– реализацию правил разграничения доступа во внешней ИС, введение ограничений на действия пользователей;

– определение обязанностей пользователей и локальных администраторов по реализации во внешней ИС мер защиты информации;

– разработку документов, определяющих правила и процедуры обеспечения безопасности обрабатываемой информации (разработка организационно-распорядительной документации);

– ознакомление работников, имеющих доступ ко внешней ИС, с положениями организационно-распорядительной документации, а также с положениями законодательства

РФ, нормативных документов ФСТЭК России и ФСБ России в области защиты информации ограниченного доступа;

– разработку технического паспорта внешней ИС.

4.3. Установка и настройка средств защиты информации

Работы по установке, монтажу, запуску и первоначальной настройке СЗИ должны выполняться в соответствии с эксплуатационной документацией на данные средства, нормативно-техническими и методическими документами уполномоченных органов исполнительной власти РФ в области обеспечения безопасности информации.

Для установки и настройки СЗИ в соответствии с законодательством РФ могут привлекаться организации, имеющие:

– лицензию ФСТЭК России на деятельность по технической защите конфиденциальной информации, позволяющую выполнять работы по контролю защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации, проведения аттестационных испытаний и аттестации на соответствие требованиям по защите информации, проектирования в защищенном исполнении средств и систем информатизации, установки и монтажа средств защиты информации;

– лицензию ФСБ России на деятельность по распространению шифровальных/криптографических средств, техническому обслуживанию шифровальных/криптографических средств, а также оказанию услуг в области шифрования информации.

По результатам установки и настройки СЗИ должны быть составлены:

– акт установок и настроек средств защиты информации;

– акт инструктажа пользователей;

– протокол настроек системы защиты информации на объекте информатизации;

– протокол фиксации исходного состояния программных компонентов средств защиты информации на объекте информатизации.

Эксплуатация СЗИ должна осуществляться в соответствии с организационно-технической, организационно-распорядительной и эксплуатационной документацией на систему защиты информации внешней ИС.

4.4. Обучение пользователей внешней ИС правилам работы с СЗИ

Ответственный за защиту информации во внешней ИС организует обучение пользователей ИС правилам работы с СЗИ. В организации-заявителе должно быть организовано ведение журнала обучения сотрудников в области защиты информации и журнала, содержащего результаты проверок осведомленности сотрудников в области защиты информации.

4.5. Проведение анализа уязвимостей внешней ИС

Для внешней ИС необходимо проведение анализа уязвимостей, который включает в себя анализ уязвимостей средств защиты информации, технических средств и программного обеспечения внешней ИС.

4.6. Мероприятия по оценке соответствия принятых мер защиты информации требованиям по защите информации во внешней ИС

Оценка эффективности принимаемых мер защиты информации во внешней ИС проводится в форме аттестации на соответствие требованиям по защите информации по

третьему классу защищенности и по обеспечению третьего уровня защищенности персональных данных.

В ходе мероприятий по оценке соответствия принятых мер защиты информации разрабатывается Программа и методики аттестационных испытаний объекта информатизации и Протокол аттестационных испытаний.

Результаты аттестационных мероприятий оформляются Заключением о результатах проведения аттестационных испытаний ИС на соответствие требованиям по защите информации. В случае, если в ходе испытаний было установлено соответствие требованиям по защите информации, приведенным в Программе и методиках аттестационных испытаний объекта информатизации, выдается Аттестат соответствия требованиям по защите информации.

4.7. Запрос на подключение к ТИС СПГ

Организация-заявитель направляет в адрес министерства труда и социального развития Новосибирской области:

– заявку на подключение к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (Приложение № 3);

– копии документов по результатам проведения работ в соответствии с п. 4.3-4.6 настоящего регламента:

- технический паспорт или иной документ, содержащий сведения о составе и размещении технических средств, входящих в состав ИС, подключаемой к ГИС;
- протокол настройки или иной документ, описывающий произведенные настройки средств защиты информации;
- отчет по результатам проведения анализа защищенности (отчет по сканированию)/протокол/акт по результатам проведения анализа защищенности;
- программа и методики аттестационных испытаний;
- протоколы аттестационных испытаний;
- заключение по результатам аттестационных испытаний;
- аттестат соответствия требованиям по защите информации.

– заверенную копию лицензии на право пользования ПО ViPNet Client;

– наименование сетевого узла ViPNet, номер сети, копию заключения о допуске пользователя СКЗИ к самостоятельной работе.

4.8. Заключение Соглашения о взаимодействии

Между министерством труда и социального развития Новосибирской области и подключаемой организацией необходимо заключить Соглашение о взаимодействии при организации работы в государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (Приложение № 5).

5. Технические условия по подключению к ТИС СПГ

В целях реализации информационного взаимодействия внешней ИС с ТИС СПГ организация-заявитель выбирает одну из нижеуказанных схем подключения к защищенной ViPNet-сети № 985.

5.1. Подключение с использованием программного комплекса «ViPNet Client»

Подключение организации-заявителя к защищенной ViPNet-сети № 985 Правительства Новосибирской области осуществляется через АРМ внешней ИС организации-заявителя, на котором установлен программный комплекс «ViPNet Client».

Типовая схема реализации варианта подключения № 1 приведена на рисунке 1.

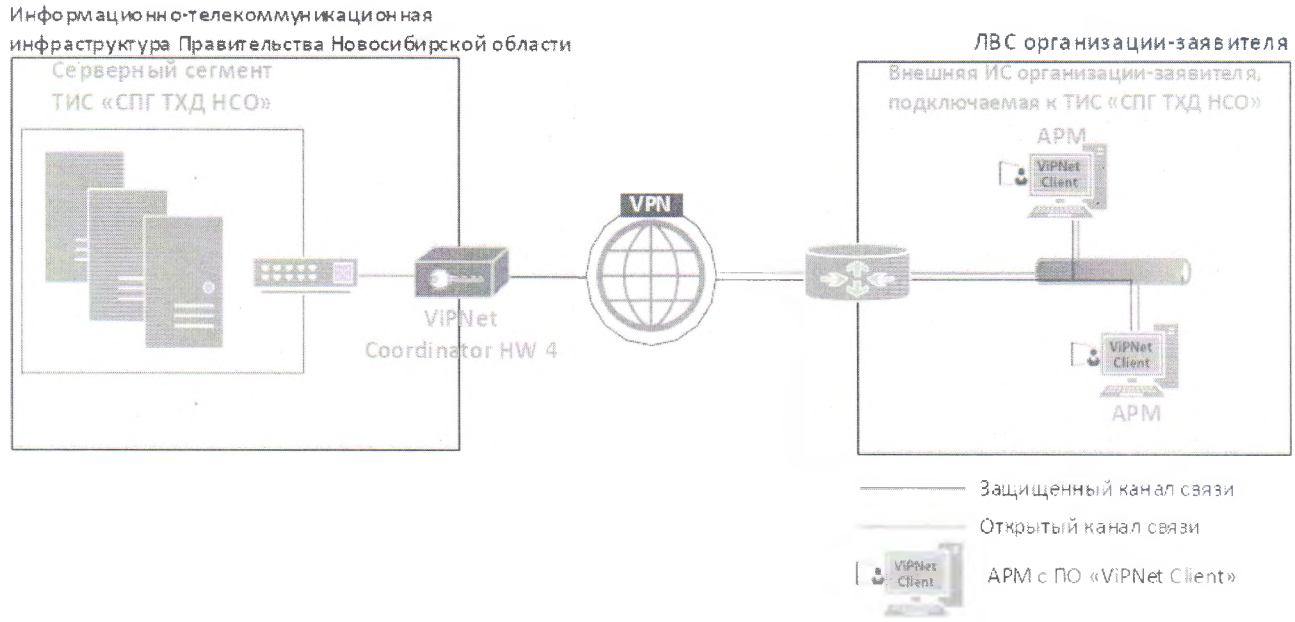

Рисунок 1 – Схема подключения № 1 (подключение с использованием ПК «ViPNet Client»)

На АРМ, входящих в состав внешней ИС, подключаемой к ТИС СПГ, должен быть установлен и настроен программный комплекс «ViPNet Client» в соответствии с требованиями и рекомендациями эксплуатационной документации производителя.

5.2. Подключение с использованием программно-аппаратного комплекса «ViPNet Coordinator HW 4»

Подключение организации-заявителя к защищенной ViPNet-сети № 985 Правительства Новосибирской области осуществляется через программно-аппаратный комплекс «ViPNet Coordinator HW 4».

Типовая схема реализации варианта подключения № 2 приведена на рисунке 2.

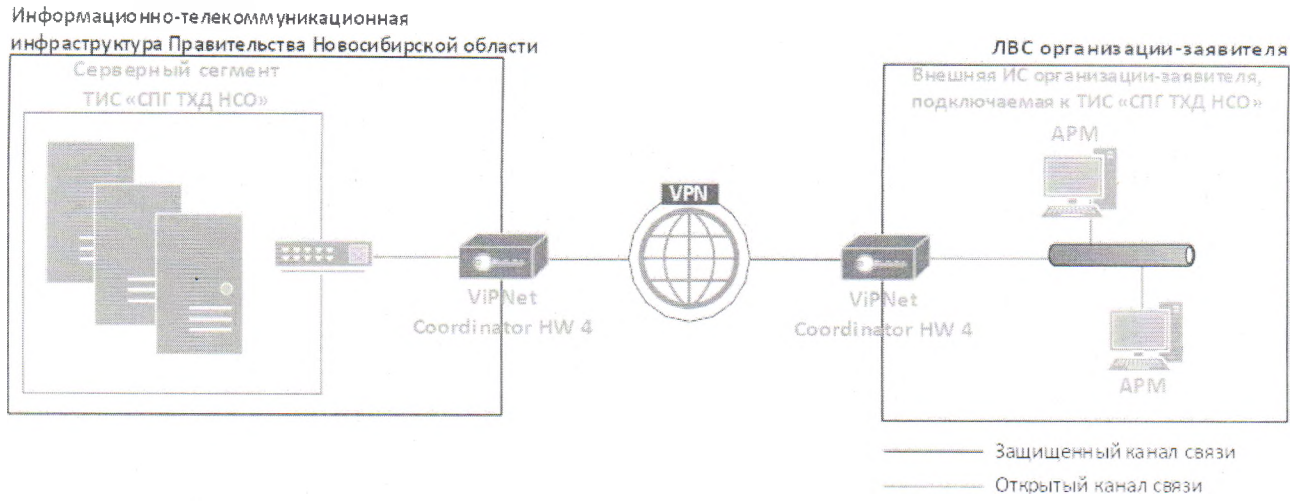

Рисунок 2 – Схема подключения № 2 (подключение с использованием ПАК «ViPNet Coordinator HW 4»)

Для реализации схемы № 2 предполагается подключение по открытой (незащищенной) локальной сети между АРМ организации-заявителя, входящими в состав внешней ИС, подключаемой к ТИС «СПГ ТХД, до ПАК «ViPNet Coordinator HW 4», установленным на стороне организации-заявителя. Размещение АРМ и ПАК «ViPNet Coordinator HW 4» на стороне организации-заявителя должно быть организовано в пределах одной контролируемой зоны.

В случае невозможности размещения АРМ и ПАК «ViPNet Coordinator HW 4» в пределах одной контролируемой зоны рекомендуется реализация схемы подключения № 1 или схемы подключения № 2.1, представленной на рисунке 3.

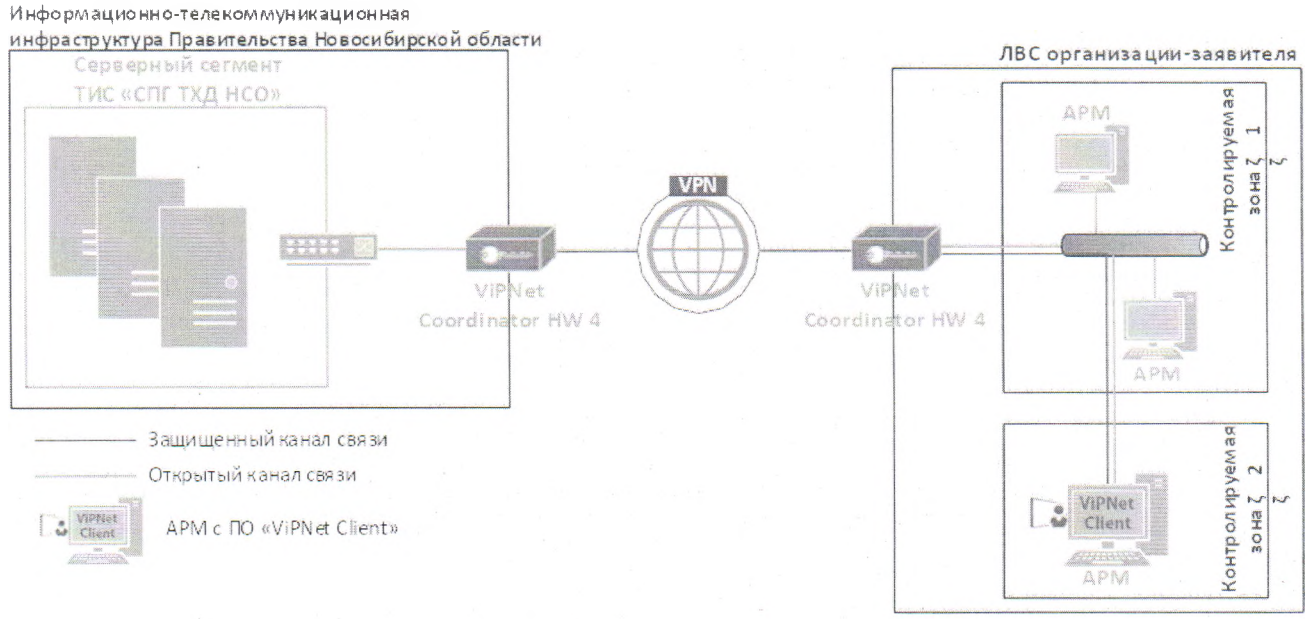

Рисунок 3– Схема подключения № 2.1

ПАК «ViPNet Coordinator HW 4» выделяется из состава защищенной ViPNet-сети № 985 по заявке организации-заявителя.

Исполнение и аппаратная платформа выделяемого ПАК «ViPNet Coordinator HW 4» определяются количеством АРМ и предполагаемой нагрузкой на внешнюю ИС.

5.3. Подключение через существующие (коммерческие) сети ViPNet с установленным межсетевым взаимодействием с сетью ViPNet Правительства Новосибирской области

Данный вариант используется в случае необходимости подключения организации-заявителя через стороннюю (в том числе коммерческую) сеть ViPNet, у которой уже имеется установленное межсетевое взаимодействие с защищенной ViPNet-сетью № 985.

Схема организации межсетевого взаимодействия сети ViPNet сторонней организации с ViPNet-сетью № 985 Правительства Новосибирской области приведена на рисунке 4.

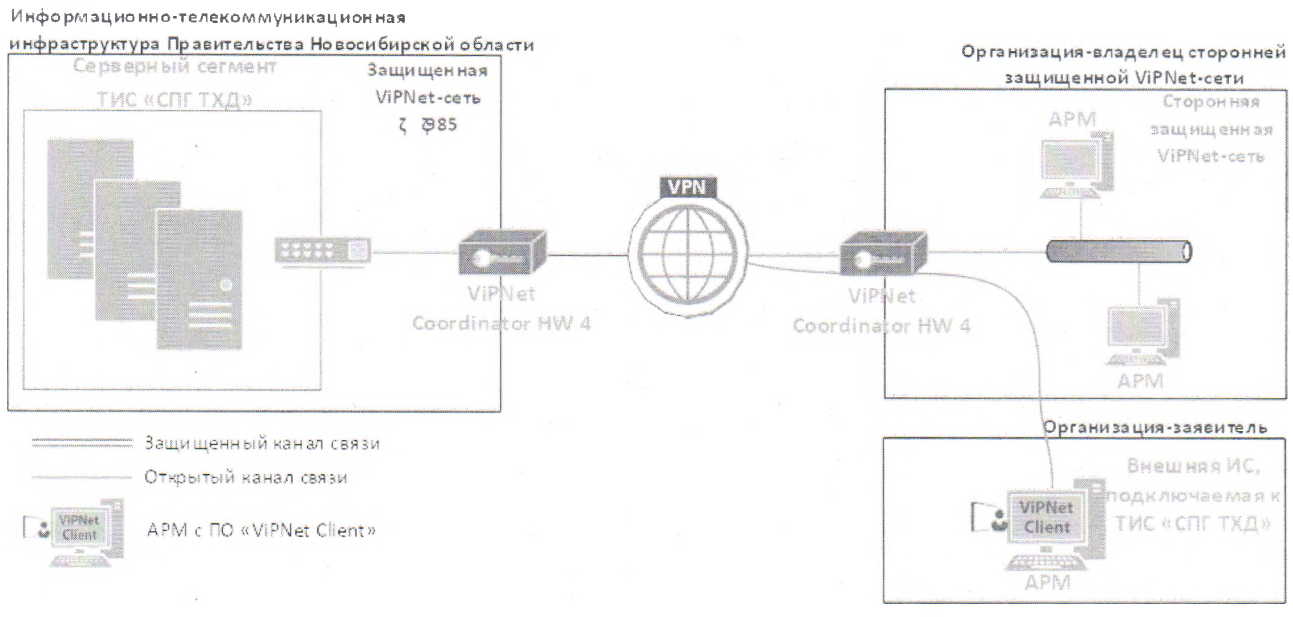

Рисунок 4 – Схема подключения № 3 (подключение через существующие (коммерческие) сети ViPNet)

В зависимости от реализации лицензия на ПК «ViPNet Client» и (или) ПАК «ViPNet Coordinator HW 4» приобретаются за счет средств организации-заявителя в стороннюю сеть ViPNet, через которую предполагается подключение к ViPNet-сети № 985. Техническое сопровождение ПК «ViPNet Client» и (или) ПАК «ViPNet Coordinator HW 4» осуществляются по договоренности между организацией-заявителем и организацией, сопровождающей стороннюю сеть.

5.4. Подключение путем организации межсетевого взаимодействия между ViPNet-сетью, принадлежащей организации-заявителю, и ViPNet-сетью № 985 Правительства Новосибирской области

Данный вариант используется в случае необходимости организации межсетевого взаимодействия существующей сети ViPNet организации-заявителя, являющейся владельцем данной сети ViPNet, с защищенной сетью ViPNet № 985 Правительства Новосибирской области. Работы по организации и дальнейшему сопровождению межсетевого взаимодействия проводятся в соответствии с эксплуатационной документацией на продуктовую линейку ViPNet силами сторон, обслуживающих соответствующие сети ViPNet.

Схема организации межсетевого взаимодействия сети ViPNet организации-заявителя с ViPNet -сетью № 985 Правительства Новосибирской области приведена на рисунке 5.

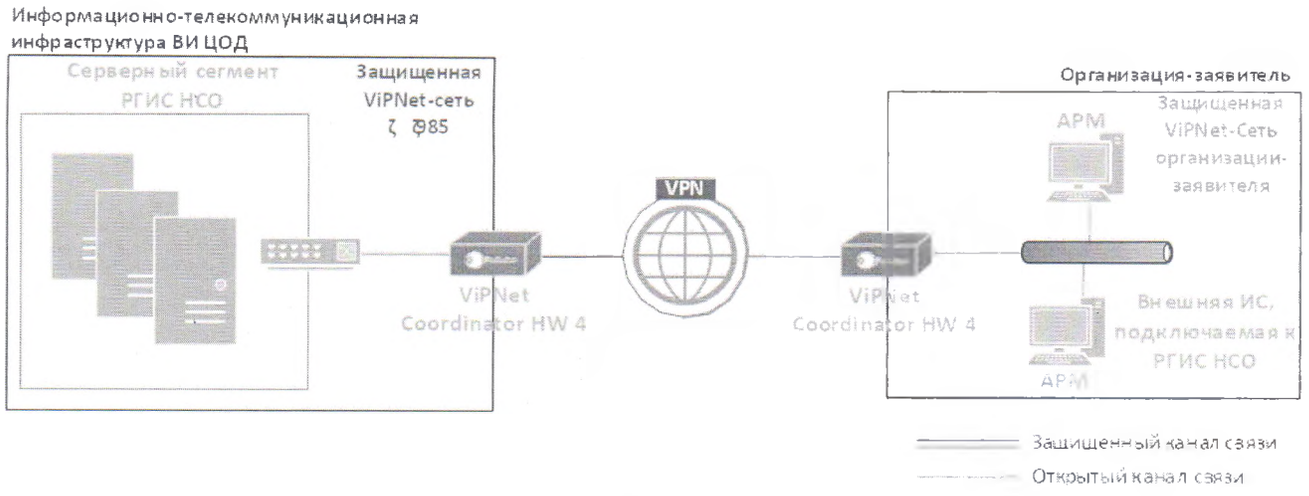

Рисунок 5 – Схема подключения № 4

6. Контроль реализации подключения к ТИС СПГ

Ответственность за соблюдение требований настоящего Регламента и обеспечение защиты информации, а также за соблюдение требований к эксплуатации СЗИ, используемых во внешних ИС, лежит на организации-заявителе, являющейся владельцем внешней ИС.

В случае выявления нарушений требований по защите информации в организации-заявителе, министерство труда и социального развития Новосибирской области уполномочено направить запрос на отключение соответствующей внешней ИС от информационных ресурсов ТИС СПГ с уведомлением руководства организации-заявителя, ответственной за эксплуатацию внешней ИС.

Повторное подключение внешней ИС к информационным ресурсам ТИС СПГ производится после документального подтверждения устранения нарушений требований по защите информации и повторного запроса на подключение.

Приложение № 1

Перечень нормативных правовых документов

1. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

3. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении Требований к защите персональных данных при их обработке в информационных системах персональных данных».

4. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».

5. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

6. Приказ ФСБ России от 18.03.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств».

7. Приказ ФАПСИ России от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».

8. Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

9. Методический документ ФСТЭК России от 11.02.2014 «Меры защиты информации в государственных информационных системах».

Приложение № 2

Сведения о реализации мер защиты информации в государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области»

Для реализации мер защиты информации во внешней ИС должны применяться следующие средства защиты информации:

- средство защиты информации от несанкционированного доступа и/или сертифицированная ФСТЭК России ОС (СЗИ от НСД);
- средство антивирусной защиты (САВЗ);
- средство обнаружения вторжений (СОВ);
- средство анализа защищенности (САНЗ);
- межсетевой экран (МЭ);
- средство защиты виртуальной инфраструктуры (СЗИ ВИ);
- средство криптографической защиты информации (СКЗИ);
- машинный носитель аутентификационной информации (Токен).

Сведения о реализации мер защиты информации в сегментах ТИС СПГ представлены в таблице 1.
Пример средств защиты информации, необходимых к применению во внешних ИС, представлен в таблице 2.

Таблица 1 – Сведения о реализации мер защиты информации

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)			

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	При доступе в ИС должна осуществляться идентификация и аутентификация внутренних пользователей, и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей. К внутренним пользователям относятся должностные лица (пользователи, администраторы), выполняющие свои должностные обязанности (функции) с использованием информации, информационных технологий и технических средств ИС в соответствии с утвержденными должностными регламентами (инструкциями), и которым в ИС присвоены учетные записи. В качестве внутренних пользователей дополнительно рассматриваются должностные лица обладателя информации, заказчика, уполномоченного лица и (или) оператора иной ИС, а также лица, привлекаемые на договорной основе для обеспечения функционирования ИС (ремонт, гарантийное обслуживание, регламентные и иные работы) в соответствии с организационно-распорядительными документами и которым в ИС также присвоены учетные записи. Пользователи ИС должны однозначно идентифицироваться и аутентифицироваться для всех видов доступа, кроме тех видов доступа, которые определяются как действия, разрешенные до идентификации и аутентификации в соответствии с мерой защиты информации УПД.11. Аутентификация пользователя осуществляется с использованием паролей, аппаратных средств, иных средств или в случае многофакторной (двухфакторной) аутентификации – определенной комбинации указанных средств. В ИС должна быть обеспечена возможность однозначного сопоставления идентификатора пользователя с запускаемыми от его имени процессами	СЗИ от НСД Токен
ИАФ.2	Идентификация устройств, в том числе стационарных, мобильных и портативных	В ИС до начала информационного взаимодействия (передачи защищаемой информации от устройства к устройству) должна осуществляться идентификация устройств (технических средств). Оператором должен быть определен перечень типов устройств, используемых в ИС и подлежащих идентификации до начала информационного взаимодействия. Идентификация устройств в ИС обеспечивается по логическим именам (имя устройства и (или) ID), логическим адресам (например, IP-адресам) и (или) по физическим адресам (например, MAC-адресам) устройства или по комбинации имени, логического и (или) физического адресов устройства	СЗИ от НСД МЭ СКЗИ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	Должно быть определено должностное лицо (администратор), ответственное за создание, присвоение и уничтожение идентификаторов пользователей и устройств. Должны быть установлены и реализованы следующие функции управления идентификаторами пользователей и устройств в ИС: – формирование идентификатора, который однозначно идентифицирует пользователя и (или) устройство; – присвоение идентификатора пользователю и (или) устройству; – предотвращение повторного использования идентификатора пользователя и (или) устройства в течение установленного периода времени; – блокирование идентификатора пользователя после установленного времени неиспользования	СЗИ от НСД
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	Должно быть определено должностное лицо (администратор), ответственное за хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации. Должны быть установлены и реализованы следующие функции управления средствами аутентификации (аутентификационной информацией) пользователей и устройств в ИС: – изменение аутентификационной информации (средств аутентификации), заданных их производителями и (или) используемых при внедрении системы защиты информации ИС; – выдача средств аутентификации пользователям; – генерация и выдача начальной аутентификационной информации (начальных значений средств аутентификации); – установление характеристик пароля (при использовании в ИС механизмов аутентификации на основе пароля); – блокирование (прекращение действия) и замена утерянных, скомпрометированных или поврежденных средств аутентификации; – назначение необходимых характеристик средств аутентификации (в том числе механизма пароля); – обновление аутентификационной информации (замена средств аутентификации) с установленной периодичностью; – защита аутентификационной информации от неправомерных доступа к ней и модифицирования	СЗИ от НСД

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	В ИС должна осуществляться защита аутентификационной информации в процессе ее ввода для аутентификации от возможного использования лицами, не имеющими на это полномочий. Защита обратной связи «система - субъект доступа» в процессе аутентификации обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации и (или) количества вводимых пользователем символов аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками	СЗИ от НСД
II. Управление доступом субъектов доступа к объектам доступа (УПД)			
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	Должны быть установлены и реализованы следующие функции управления учетными записями пользователей: – определение типа учетной записи (внутреннего пользователя, внешнего пользователя; системная, приложения; гостевая (анонимная), временная и (или) иные типы записей); – объединение учетных записей в группы (при необходимости); – верификация пользователя (проверка личности пользователя, его должностных (функциональных) обязанностей) при заведении учетной записи пользователя; – заведение, активация, блокирование и уничтожение учетных записей пользователей; – пересмотр и, при необходимости, корректировка учетных записей пользователей с установленной периодичностью; – порядок заведения и контроля использования гостевых (анонимных) и временных учетных записей пользователей, а также привилегированных учетных записей администраторов; – оповещение администратора, осуществляющего управление учетными записями пользователей, об изменении сведений о пользователях, их ролях, обязанностях, полномочиях, ограничениях; – уничтожение временных учетных записей пользователей, предоставленных для однократного (ограниченного по времени) выполнения задач в информационной системе; – предоставление пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами	СЗИ от НСД

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	В ИС для управления доступом субъектов доступа к объектам доступа должны быть реализованы методы управления доступом, назначены типы доступа субъектов к объектам доступа и реализованы правила разграничения доступа субъектов доступа к объектам доступа. Методы управления доступом реализуются в зависимости от особенностей функционирования ИС, с учетом угроз безопасности информации и должны включать один или комбинацию следующих методов: – дискреционный метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе идентификационной информации субъекта и для каждого объекта доступа – списка, содержащего набор субъектов доступа (групп субъектов) и ассоциированных с ними типов доступа; – ролевой метод управления доступом, предусматривающий управление доступом субъектов доступа к объектам доступа на основе ролей субъектов доступа (совокупность действий и обязанностей, связанных с определенным видом деятельности). Правила разграничения доступа реализуются на основе установленных списков доступа или матриц доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа	СЗИ от НСД
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	В ИС должно осуществляться управление информационными потоками при передаче информации между устройствами, сегментами в рамках ИС, включающее: – фильтрацию информационных потоков в соответствии с установленными правилами управления потоками; – разрешение передачи информации в ИС только по установленному маршруту; – изменение (перенаправление) маршрута передачи информации в установленных случаях; – запись во временное хранилище информации для анализа и принятия решения о возможности ее дальнейшей передачи в установленных случаях. Управление информационными потоками должно обеспечивать разрешенный маршрут прохождения информации между пользователями, устройствами, сегментами в рамках ИС, а также между ИС или при взаимодействии с сетью Интернет (или другими информационно-телекоммуникационными сетями международного информационного обмена) на основе правил управления информационными	МЭ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		потоками, включающих контроль конфигурации информационной системы, источника и получателя передаваемой информации, структуры передаваемой информации, характеристик информационных потоков и (или) канала связи (без анализа содержания информации). Управление информационными потоками должно блокировать передачу защищаемой информации через сеть Интернет по незащищенным линиям связи, сетевые запросы и трафик, несанкционированно исходящие из ИС и (или) входящие в ИС	
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	Должно быть обеспечено разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, в соответствии с их должностными обязанностями (функциями), фиксирование в организационно-распорядительных документах по защите информации (документирование) полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, и санкционирование доступа к объектам доступа в соответствии с разделением полномочий (ролей)	СЗИ от НСД
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	Должны быть однозначно определены и зафиксированы в организационно-распорядительных документах по защите информации (задокументированы) роли и (или) должностные обязанности (функции), также объекты доступа, в отношении которых установлен наименьший уровень привилегий. Доступ к объектам доступа с учетом минимально необходимых прав и привилегий обеспечивается в соответствии с УПД.2	СЗИ от НСД
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	В ИС должно быть установлено и зафиксировано в организационно-распорядительных документах по защите информации (задокументировано) ограничение количества неуспешных попыток входа в ИС (доступа к информационной системе) за установленный период времени, а также обеспечено блокирование устройства, с которого предпринимаются попытки доступа, и (или) учетной записи пользователя при превышении пользователем ограничения количества неуспешных попыток входа в информационную систему (доступа к ИС). Ограничение количества неуспешных попыток входа в ИС (доступа к ИС) должно обеспечиваться в соответствии с ИАФ.4	СЗИ от НСД
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия	В ИС должно обеспечиваться блокирование сеанса доступа пользователя после установленного времени его бездействия (неактивности) в ИС или по запросу пользователя. Блокирование сеанса доступа пользователя в ИС обеспечивает временное приостановление работы пользователя со средством вычислительной техники, с которого осуществляется доступ к ИС (без выхода из ИС).	СЗИ от НСД

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
	(неактивности) пользователя или по его запросу	Для заблокированного сеанса должно осуществляться блокирование любых действий по доступу к информации и устройствам отображения, кроме необходимых для разблокирования сеанса. Блокирование сеанса доступа пользователя в ИС должно сохраняться до прохождения им повторной идентификации и аутентификации	
УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации	Должен быть установлен перечень действий пользователей, разрешенных до прохождения ими процедур идентификации и аутентификации, и запрет действий пользователей, не включенных в перечень разрешенных действий, до прохождения ими процедур идентификации и аутентификации. Администратору разрешаются действия в обход установленных процедур идентификации и аутентификации, необходимые только для восстановления функционирования ИС в случае сбоев в работе или выходе из строя отдельных технических средств (устройств)	СЗИ от НСД
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	Должна обеспечиваться защита информации при доступе пользователей (процессов запускаемых от имени пользователей) и (или) иных субъектов доступа к объектам доступа ИС через ИТКС, с использованием стационарных и (или) мобильных технических средств. Защита удаленного доступа должна обеспечиваться при всех видах доступа и включать: – установление видов доступа, разрешенных для удаленного доступа к объектам доступа информационной системы; – ограничение на использование удаленного доступа в соответствии с задачами ИС, для решения которых такой доступ необходим, и предоставление удаленного доступа для каждого разрешенного вида удаленного доступа в соответствии с УПД.2; – предоставление удаленного доступа только тем пользователям, которым он необходим для выполнения установленных должностных обязанностей (функций); – мониторинг и контроль удаленного доступа на предмет выявления несанкционированного удаленного доступа к объектам доступа ИС	МЭ СКЗИ
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств [1]	Должны обеспечиваться регламентация и контроль использования в ИС мобильных технических средств, направленные на защиту информации в ИС. Регламентация и контроль использования мобильных технических средств должны включать: – установление (в том числе документальное) видов доступа, разрешенных для доступа к объектам доступа ИС с использованием мобильных технических средств, входящих в состав ИС;	СЗИ от НСД

[1] Актуальна в случае применения мобильных технических средств во внешних ИС, подключенных к ТИС СПГ.

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		– использование в составе ИС для доступа к объектам доступа мобильных технических средств (служебных мобильных технических средств), в которых реализованы меры защиты информации; – ограничение на использование мобильных технических средств в соответствии с задачами (функциями) ИС, для решения которых использование таких средств необходимо, и предоставление доступа с использованием мобильных технических средств; – мониторинг и контроль применения мобильных технических средств на предмет выявления несанкционированного использования мобильных технических средств для доступа к объектам доступа информационной системы; – запрет возможности запуска без команды пользователя в информационной системе программного обеспечения (программного кода), используемого для взаимодействия с мобильным техническим средством	
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	Должно быть обеспечено управление взаимодействием с внешними ИС, включающими ИС и вычислительные ресурсы (мощности) уполномоченных лиц, ИС, с которыми установлено информационное взаимодействие на основании заключенного договора (соглашения), а также с иными ИС, информационное взаимодействие с которыми необходимо для функционирования ИС. Управление взаимодействием с внешними ИС должно включать: – предоставление доступа к ИС только авторизованным (уполномоченным) пользователям; – определение типов прикладного программного обеспечения ИС, к которым разрешен доступ авторизованным (уполномоченным) пользователям из внешних ИС; – определение системных учетных записей, используемых в рамках данного взаимодействия; – определение порядка предоставления доступа к ИС авторизованными (уполномоченным) пользователями из ИС; – определение порядка обработки, хранения и передачи информации с использованием внешних ИС	МЭ СКЗИ
III. Ограничение программной среды (ОПС)			
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих	Оператором должны быть реализованы следующие функции по управлению установкой (инсталляцией) компонентов программного обеспечения ИС: – определение компонентов программного обеспечения (состава и конфигурации), подлежащих установке в ИС после загрузки операционной системы; – настройка параметров установки компонентов ПО, обеспечивающая исключение установки (если	Обеспечивается принятием организационных мер защиты информации

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
	установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения	осуществимо) компонентов программного обеспечения, использование которых не требуется для реализации информационной технологии ИС; – контроль за установкой компонентов ПО (состав компонентов, параметры установки, конфигурация компонентов); – определение и применение параметров настройки компонентов ПО, включая программные компоненты СЗИ, обеспечивающих реализацию мер ЗИ, а также устранение возможных уязвимостей ИС, приводящих к возникновению угроз безопасности информации	
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов	Должна быть обеспечена установка (инсталляция) только разрешенного к использованию в ИС программного обеспечения и (или) его компонентов. Установка (инсталляция) в ИС программного обеспечения (вида, типа, класса программного обеспечения) и (или) его компонентов осуществляется с учетом перечня программного обеспечения и (или) его компонентов, разрешенных к установке («белый список»), и (или) перечнем программного обеспечения и (или) его компонентов, запрещенных к установке («черный список»). Указанные перечни программного обеспечения и (или) его компонентов разрабатываются для ИС в целом или для всех ее сегментов или устройств в отдельности и фиксируются в организационно-распорядительной документации по защите информации (документируются). Установка (инсталляция) в ИС программного обеспечения и (или) его компонентов должна осуществляться только от имени администратора в соответствии с УПД.5. Должен обеспечиваться периодический контроль установленного (инсталлированного) в ИС программного обеспечения на предмет соответствия его перечню программного обеспечения, разрешенному к установке в ИС в соответствии с АНЗ.4, а также на предмет отсутствия программного обеспечения, запрещенного к установке	Обеспечивается принятием организационных мер защиты информации
IV. Защита машинных носителей информации (ЗНИ)			
ЗНИ.1	Учет машинных носителей информации	Должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учету подлежат: – съемные машинные носители информации; – портативные вычислительные устройства, имеющие встроенные носители информации; – машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках). Учет машинных носителей информации включает присвоение регистрационных (учетных) номеров	Обеспечивается принятием организационных мер защиты информации

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		носителям. В качестве регистрационных номеров могут использоваться идентификационные (серийные) номера машинных носителей, присвоенных производителями этих машинных носителей информации, номера инвентарного учета, в том числе инвентарные номера технических средств, имеющих встроенные носители информации, и иные номера. Регистрационные или иные номера подлежат занесению в журналы учета машинных носителей информации или журналы материально-технического учета с указанием пользователя или группы пользователей, которым разрешен доступ к машинным носителям информации	
ЗНИ.2	Управление доступом к машинным носителям информации	Должны быть реализованы следующие функции по управлению доступом к машинным носителям информации, используемым в ИС: – определение должностных лиц, имеющих физический доступ к машинным носителям информации; – предоставление физического доступа к машинным носителям информации только тем лицам, которым он необходим для выполнения своих должностных обязанностей (функций)	Обеспечивается принятием организационных мер защиты информации
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители информации	В ИС должен осуществляться контроль использования интерфейсов ввода (вывода). Контроль использования (разрешение или запрет) интерфейсов ввода (вывода) должен предусматривать: – определение оператором интерфейсов средств вычислительной техники, которые могут использоваться для ввода (вывода) информации, разрешенных и (или) запрещенных к использованию в информационной системе; – определение оператором категорий пользователей, которым предоставлен доступ к разрешенным к использованию интерфейсов ввода (вывода); – принятие мер, исключающих возможность использования запрещенных интерфейсов ввода (вывода); – контроль доступа пользователей к разрешенным к использованию интерфейсов ввода (вывода)	СЗИ от НСД
ЗНИ.8	Уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания)	Должно обеспечиваться уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) информации. Уничтожение (стирание) информации на машинных носителях должно исключать возможность восстановления защищаемой информации при передаче машинных носителей между пользователями, в сторонние организации для ремонта или утилизации. Уничтожению (стиранию) подлежит информация, хранящаяся на цифровых и нецифровых, съемных и несъемных машинных носителях информации	СЗИ от НСД

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
V. Регистрация событий безопасности (РСБ)			
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	Должны быть определены события безопасности в ИС, подлежащие регистрации, и сроки их хранения. К событиям безопасности, подлежащим регистрации в ИС, должны быть отнесены любые проявления состояния ИС и ее системы защиты информации, указывающие на возможность нарушения конфиденциальности, целостности или доступности информации, доступности компонентов ИС, нарушения процедур, установленных организационно-распорядительными документами по защите информации, а также на нарушение штатного функционирования средств защиты информации. События безопасности, подлежащие регистрации в ИС, и сроки их хранения соответствующих записей регистрационных журналов должны обеспечивать возможность обнаружения, идентификации и анализа инцидентов, возникших в информационной системе. Подлежат регистрации события безопасности, связанные с применением выбранных мер по защите информации в ИС	СЗИ от НСД САВЗ МЭ СКЗИ
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	В ИС должны быть определены состав и содержание информации о событиях безопасности, подлежащих регистрации. Состав и содержание информации о событиях безопасности, включаемой в записи регистрации о событиях безопасности, должны, как минимум, обеспечить возможность идентификации типа события безопасности, даты и времени события безопасности, идентификационной информации источника события безопасности, результат события безопасности (успешно или неуспешно), субъект доступа (пользователь и (или) процесс), связанный с данным событием безопасности	СЗИ от НСД САВЗ МЭ СКЗИ
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	В ИС должны осуществляться сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения информации о событиях безопасности. Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения должны предусматривать: – возможность выбора администратором безопасности событий безопасности, подлежащих регистрации в текущий момент времени из перечня событий безопасности, определенных в соответствии с РСБ.1; – генерацию (сбор, запись) записей регистрации (аудита) для событий безопасности, подлежащих регистрации (аудиту) в соответствии с РСБ.1 с составом и содержанием информации, определенными в соответствии с РСБ.2; – хранение информации о событиях безопасности в течение времени, установленного в соответствии с РСБ.1	СЗИ от НСД САВЗ МЭ СКЗИ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти	В ИС должно осуществляться реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти. Реагирование на сбои при регистрации событий безопасности должно предусматривать: – предупреждение (сигнализация, индикация) администраторов о сбоях (аппаратных и программных ошибках, сбоях в механизмах сбора информации или переполнения объема (емкости) памяти) при регистрации событий безопасности; – реагирование на сбои при регистрации событий безопасности путем изменения администраторами параметров сбора, записи и хранения информации о событиях безопасности, в том числе отключение записи информации о событиях безопасности от части компонентов ИС, запись поверх устаревших хранимых записей событий безопасности	СЗИ от НСД САВЗ МЭ СКЗИ
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них	Должен осуществляться мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Мониторинг (просмотр и анализ) записей регистрации (аудита) должен проводиться для всех событий, подлежащих регистрации в соответствии с РСБ.1, и с установленной периодичностью, обеспечивающей своевременное выявление признаков инцидентов безопасности в информационной системе. В случае выявление признаков инцидентов безопасности в ИС должны осуществляться планирование и проведение мероприятий по реагированию на выявленные инциденты безопасности	СЗИ от НСД САВЗ МЭ СКЗИ
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе	В ИС должно осуществляться генерирование надежных меток времени и (или) синхронизация системного времени. Получение меток времени, включающих дату и время, используемых при генерации записей регистрации (аудита) событий безопасности в ИС достигается посредством применения внутренних системных часов информационной системы	–
РСБ.7	Защита информации о событиях безопасности	Защита информации о событиях безопасности (записях регистрации (аудита)) обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, и в том числе включает защиту средств ведения регистрации (аудита) и настроек механизмов регистрации событий. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам	СЗИ от НСД САВЗ МЭ СКЗИ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
VI. Антивирусная защита (АВЗ)			
АВЗ.1	Реализация антивирусной защиты	Реализация антивирусной защиты должна предусматривать: – применение средств антивирусной защиты на АРМ, серверах, периметральных СЗИ (средствах межсетевого экранирования, прокси-серверах, почтовых шлюзах и других СЗИ), мобильных технических средствах и иных точках доступа в информационную систему, подверженных внедрению (заражению) вредоносными компьютерными программами (вирусами) через съемные машинные носители информации или сетевые подключения, в том числе к сетям общего пользования (вложения электронной почты, веб- и другие сетевые сервисы); – установку, конфигурирование и управление средствами антивирусной защиты; – предоставление доступа средствам антивирусной защиты к объектам ИС, которые должны быть подвергнуты проверке средством антивирусной защиты; – проведение периодических проверок компонентов ИС (АРМ, серверов, других средств вычислительной техники) на наличие вредоносных компьютерных программ (вирусов); – проверку в масштабе времени, близком к реальному, объектов (файлов) из внешних источников (съемных МНИ, сетевых подключений, в том числе к сетям общего пользования, и других внешних источников) при загрузке, открытии или исполнении таких файлов; – оповещение администраторов безопасности в масштабе времени, близком к реальному, об обнаружении вредоносных компьютерных программ (вирусов); – определение и выполнение действий по реагированию на обнаружение в ИС объектов, подвергшихся заражению вредоносными компьютерными программами (вирусами)	САВЗ
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	Обновление базы данных признаков вредоносных компьютерных программ (вирусов) должно предусматривать: – получение уведомлений о необходимости обновлений и непосредственном обновлении базы данных признаков вредоносных компьютерных программ (вирусов); – получение из доверенных источников и установку обновлений базы данных признаков вредоносных компьютерных программ (вирусов); – контроль целостности обновлений базы данных признаков вредоносных компьютерных программ (вирусов)	
VII. Обнаружение вторжений (СОВ)			
СОВ.1	Обнаружение вторжений	Оператором должно обеспечиваться обнаружение (предотвращение) вторжений (компьютерных атак),	СОВ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней, с использованием систем обнаружения вторжений. Обнаружение (предотвращение) вторжений должно осуществляться на внешней границе ИС (системы обнаружения вторжений уровня сети) и (или) на внутренних узлах (системы обнаружения вторжений уровня узла) сегментов информационной системы (автоматизированных рабочих местах, серверах и иных узлах), определяемых оператором. Права по управлению (администрированию) системами обнаружения вторжений должны предоставляться только уполномоченным должностным лицам. Системы обнаружения вторжений должны обеспечивать реагирование на обнаруженные и распознанные компьютерные атаки с учетом особенностей функционирования ИС	
СОВ.2	Обновление базы решающих правил	Оператором должно обеспечиваться обновление базы решающих правил системы обнаружения вторжений, применяемой в информационной системе. Обновление базы решающих правил системы обнаружения вторжений должно предусматривать: – получение уведомлений о необходимости обновлений и непосредственном обновлении базы решающих правил; – получение из доверенных источников и установку обновлений базы решающих правил; – контроль целостности обновлений базы решающих правил	СОВ
VIII. Контроль (анализ) защищенности информации (АНЗ)			
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей	При выявлении (поиске), анализе и устранении уязвимостей в ИС должны проводиться: – выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении средств защиты информации, правильностью установки и настройки средств защиты информации, технических средств и программного обеспечения, а также корректностью работы средств защиты информации при их взаимодействии с техническими средствами и программным обеспечением; – разработка по результатам выявления (поиска) уязвимостей отчетов с описанием выявленных уязвимостей и планом мероприятий по их устранению; – анализ отчетов с результатами поиска уязвимостей и оценки достаточности реализованных мер защиты информации; – устранение выявленных уязвимостей, в том числе путем установки обновлений программного обеспечения средств защиты информации, общесистемного программного обеспечения, прикладного	САНЗ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		программного обеспечения или микропрограммного обеспечения технических средств; – информирование должностных лиц (пользователей, администраторов, подразделения по защите информации) о результатах поиска уязвимостей и оценки достаточности реализованных мер защиты информации. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации ИС. На этапе эксплуатации поиск и анализ уязвимостей проводится с установленной периодичностью. Должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей	
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	Должен осуществляться контроль установки обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. Должно осуществляться получение из доверенных источников и установка обновлений программного обеспечения, включая программное обеспечение средств защиты информации и программное обеспечение базовой системы ввода-вывода. Контроль установки обновлений проводится с установленной в организационно-распорядительных документах по защите информации и фиксируется в соответствующих журналах	САВЗ САНЗ
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ	Должен проводиться контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации. При контроле работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации должны осуществляться: – контроль работоспособности (неотключения) программного обеспечения и средств защиты информации; – проверка правильности функционирования (тестирование на тестовых данных, приводящих к известному результату) программного обеспечения и средств защиты информации; – контроль соответствия настроек программного обеспечения и средств защиты информации параметрам настройки, приведенным в эксплуатационной документации на систему защиты информации и средства защиты информации; – восстановление работоспособности (правильности функционирования) и параметров настройки программного обеспечения и средств защиты информации (при необходимости), в том числе с использованием резервных копий и (или) дистрибутивов	СЗИ от НСД САВЗ СОВ САНЗ МЭ СКЗИ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
АНЗ.4	Контроль состава технических средств, ПО и средств защиты информации	Должен проводиться контроль состава технических средств, программного обеспечения и средств защиты информации, применяемых в ИС (инвентаризация). При контроле состава технических средств, программного обеспечения и средств защиты информации должны осуществляться: – контроль соответствия состава технических средств, программного обеспечения и средств защиты информации приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ИС и принятие мер, направленных на устранение выявленных недостатков; – контроль состава технических средств, программного обеспечения и средств защиты информации на соответствие сведениям действующей (актуализированной) эксплуатационной документации и принятие мер, направленных на устранение выявленных недостатков; – контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принятие мер, направленных на устранение выявленных недостатков; – исключение (восстановление) из состава ИС несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации. Контроль состава технических средств, программного обеспечения и средств защиты информации проводится с установленной периодичностью	СЗИ от НСД САВЗ САНЗ
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе	При контроле правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС должны осуществляться: – контроль правил генерации и смены паролей пользователей; – контроль заведения и удаления учетных записей пользователей; – контроль реализации правил разграничения доступом; – контроль реализации полномочий пользователей; – контроль наличия документов, подтверждающих разрешение изменений учетных записей пользователей, их параметров, правил разграничения доступом и полномочий пользователей, предусмотренных организационно-распорядительными документами по защите информации; – устранение нарушений, связанных с генерацией и сменой паролей пользователей, заведением и удалением учетных записей пользователей, реализацией правил разграничения доступом, установлением полномочий пользователей	СЗИ от НСД
IX. Обеспечение целостности информационной системы и информации (ОЦЛ)			

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение СЗИ	В ИС должен осуществляться контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации. Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации, должен предусматривать: – контроль целостности программного обеспечения средств защиты информации, включая их обновления, по наличию имен (идентификаторов) и (или) по контрольным суммам компонентов средств защиты информации в процессе загрузки и (или) динамически в процессе работы ИС; – контроль целостности компонентов программного обеспечения (за исключением средств защиты информации), определяемого оператором исходя из возможности реализации угроз безопасности информации, по наличию имен (идентификаторов) компонентов программного обеспечения и (или) по контрольным суммам в процессе загрузки и (или) динамически в процессе работы ИС; – контроль применения средств разработки и отладки программ в составе программного обеспечения информационной системы; – тестирование с периодичностью, установленной оператором, функций безопасности средств защиты информации, в том числе с помощью тест-программ, имитирующих попытки несанкционированного доступа, и (или) специальных программных средств; – обеспечение физической защиты технических средств ИС	СЗИ от НСД САВЗ СОВ САНЗ МЭ СКЗИ
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая ПО средств защиты информации, при возникновении нештатных ситуаций	Для обеспечения возможности восстановления программного обеспечения в ИС должны быть приняты соответствующие планы по действиям персонала (администраторов безопасности, пользователей) при возникновении нештатных ситуаций. Возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций должна предусматривать: – восстановление программного обеспечения, включая программное обеспечение средств защиты информации, из резервных копий (дистрибутивов) программного обеспечения; – восстановление и проверка работоспособности системы защиты информации, обеспечивающие необходимый уровень защищенности информации; – возврат ИС в начальное состояние (до возникновения нештатной ситуации), обеспечивающее ее штатное функционирование, или восстановление отдельных функциональных возможностей ИС, позволяющих решать задачи по обработке информации	СЗИ от НСД САВЗ МЭ СКЗИ
X. Обеспечение доступности информации (ОДТ)			
ОДТ.3	Контроль безотказного	Контроль безотказного функционирования проводится в отношении серверного и	Обеспечивается принятием

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
	функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование	телекоммуникационного оборудования, каналов связи, средств обеспечения функционирования ИС путем периодической проверки работоспособности в соответствии с эксплуатационной документацией (в том числе путем посылки тестовых сообщений и принятия «ответов», визуального контроля, контроля трафика, контроля «поведения» системы или иными методами). При обнаружении отказов функционирования осуществляется их локализация и принятие мер по восстановлению отказавших средств, их тестирование в соответствии с эксплуатационной документацией, а также регистрация событий, связанных с отказами функционирования, в соответствующих журналах	организационных мер защиты информации
XI. Защита технических средств (ЗТС)			
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования	Должна обеспечиваться контролируемая зона, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования. Контролируемая зона включает пространство (территорию, здание, часть здания), в котором исключено неконтролируемое пребывание работников (сотрудников) и лиц, не имеющих постоянного допуска на объекты ИС, а также транспортных, технических и иных материальных средств. Границы контролируемой зоны устанавливаются в организационно-распорядительных документах по защите информации	Обеспечивается принятием организационных мер защиты информации
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к	Должны обеспечиваться контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования ИС и помещения и сооружения, в которых они установлены. Контроль и управление физическим доступом должны предусматривать: – определение лиц, допущенных к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; – санкционирование физического доступа к техническим средствам, СЗИ, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены; – учет физического доступа к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены	Обеспечивается принятием организационных мер защиты информации

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
	средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и помещения и сооружения, в которых они установлены		
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	Должно осуществляться размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр. Размещение устройств вывода (отображения, печати) информации должно исключать возможность несанкционированного просмотра выводимой информации, как из-за пределов контролируемой зоны, так и в пределах контролируемой зоны	Обеспечивается принятием организационных мер защиты информации
XII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)			
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты информации, функций по обработке информации и иных функций информационной системы	В ИС должно быть обеспечено разделение функциональных возможностей по управлению (администрированию) ИС, управлению (администрированию) системой защиты информации (функций безопасности) и функциональных возможностей пользователей по обработке информации. Разделение функциональных возможностей обеспечивается на физическом и (или) логическом уровне путем выделения части программно-технических средств ИС, реализующих функциональные возможности по управлению (администрированию) ИС и управлению (администрированию) системой защиты информации, в отдельный домен, использования различных автоматизированных рабочих мест и серверов, различных типов операционных систем, разных способов аутентификации, различных сетевых адресов, выделенных каналов управления и (или) комбинаций данных способов, а также иными методами	СЗИ от НСД

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ЗИС.3	Обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	Должна быть обеспечена защита информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны. Защита информации обеспечивается путем защиты каналов связи от несанкционированного физического доступа (подключения) к ним и (или) применения в соответствии с законодательством Российской Федерации средств криптографической защиты информации	СКЗИ
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов	В ИС должно осуществляться обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов (защита от атак типа «человек посередине»). Для подтверждения подлинности сторон сетевого соединения (сеанса взаимодействия) и защиты сетевых устройств и сервисов от подмены должна осуществляться их аутентификация. Контроль целостности передаваемой информации должен включать проверку целостности передаваемых пакетов	МЭ СКЗИ
ЗИС.12	Исключение возможности отрицания пользователем факта отправки информации другому пользователю	Должно обеспечиваться исключение возможности отрицания пользователем факта отправки информации другому пользователю. Для исключения возможности отрицания пользователем факта отправки информации другому пользователю должны осуществляться: – определение объектов или типов информации, для которых требуется обеспечение неотказуемости отправки; – обеспечение целостности информации при ее подготовке к передаче и непосредственной ее передаче по каналам связи; – регистрация событий, связанных с отправкой информации другому пользователю	СКЗИ
ЗИС.13	Исключение возможности отрицания пользователем факта получения информации от другого пользователя	Должно обеспечиваться исключение возможности отрицания пользователем факта получения информации от другого пользователя. Для исключения возможности отрицания пользователем факта получения информации должны осуществляться: – определение объектов или типов информации, для которых требуется обеспечение неотказуемости	СКЗИ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
		получения; – обеспечение целостности полученной информации; – регистрация событий, связанных с получением информации от другого пользователя	
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации	В ИС должна обеспечиваться защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения, иных данных, не подлежащих изменению в процессе обработки информации. Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки информации, обеспечивается принятием мер защиты информации, определенных оператором, направленных на обеспечение их конфиденциальности и целостности. Защита данных, не подлежащих изменению в процессе обработки информации, обеспечивается в отношении информации, хранящейся на жестких магнитных дисках, дисковых накопителях и иных накопителях в ИС	СЗИ от НСД
ЗИС.22	Защита информационной системы от угроз безопасности информации, направленных на отказ в обслуживании информационной системы	В ИС должна обеспечиваться защита от угроз безопасности информации, направленных на отказ в обслуживании этой системы. Защита от угроз безопасности информации, направленных на отказ в обслуживании, должна осуществляться посредством реализации в ИС мер защиты информационной системы в соответствии с ЗИС.23 и повышенными характеристиками производительности телекоммуникационного оборудования и каналов передачи совместно с резервированием информации и технических средств, программного обеспечения, каналов передачи информации в соответствии с ОДТ.4 и ОДТ.5	МЭ СОВ
ЗИС.23	Защита периметра (физических и (или) логических границ) информационной системы при ее взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями	В ИС должна осуществляться защита периметра (физических и (или) логических границ) ИС при ее взаимодействии с иными ИС и ИТКС, предусматривающая: – управление (контроль) входящими в ИС и исходящими из ИС информационными потоками на физической и (или) логической границе ИС (сегментов ИС); – обеспечение взаимодействия ИС и (или) ее сегментов с иными информационными системами и сетями только через сетевые интерфейсы, которые обеспечивают управление (контроль) информационными потоками с использованием средств защиты информации (управляемые (контролируемые) сетевые интерфейсы), установленных на физическом и (или) логическом периметре информационной системы или ее отдельных сегментов (маршрутизаторов, межсетевых экранов, коммутаторов, прокси-серверов, шлюзов безопасности, средств построения виртуальных частных сетей и иных средств защиты информации)	МЭ

Условное обозначение и номер меры	Меры защиты информации в информационных системах	Реализация меры защиты информации	Виды и типы СЗИ, используемые для реализации технических мер защиты информации
ЗИС.24	Прекращение сетевых соединений по их завершении или по истечении заданного оператором временного интервала неактивности сетевого соединения	В информационной системе должно осуществляться завершение сетевых соединений (например, открепление пары порт/адрес (TCP/IP)) по их завершении и (или) по истечении заданного оператором временного интервала неактивности сетевого соединения	СКЗИ
ЗИС.30	Регламентация и контроль использования в информационной системе мобильных технических средств [2]	Должна осуществляться защита применяемых в ИС мобильных технических средств. Защита мобильных технических средств включает: – реализацию в зависимости от мобильного технического средства (типа мобильного технического средства) мер по идентификации и аутентификации, управлению доступом, ограничению программной среды, защите машинных носителей информации, регистрации событий безопасности, антивирусной защите, контролю (анализу) защищенности, обеспечению целостности; – очистку (удаление) информации в мобильном техническом средстве после завершения сеанса удаленного доступа к защищаемой информации или принятие иных мер, исключающих несанкционированный доступ к хранимой защищаемой информации; – уничтожение съемных машинных носителей информации, которые не подлежат очистке; – выборочные проверки мобильных технических средств (на предмет их наличия) и хранящейся на них информации (например, на предмет отсутствия информации, не соответствующей маркировке носителя информации); – запрет возможности автоматического запуска (без команды пользователя) в информационной системе программного обеспечения на мобильных технических средствах	СЗИ от НСД САВЗ САНЗ

Таблица 2 – Пример необходимых средств защиты информации

Сокращение	Расшифровка	Пример	Примечание
СЗИ от НСД	Средство защиты информации от несанкционированного доступа	Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-K»	Если не используется сертифицированная ОС
Сертифицированная ОС	Сертифицированная ФСТЭК России операционная система	Операционная система Альт 8 СП	
САВЗ	Средство антивирусной защиты	Программное изделие «Kaspersky Endpoint Security для Windows»	

[2] Актуальна в случае применения мобильных технических средств во внешних ИС, подключенных к ТИС СПГ

		Программное изделие «Kaspersky Endpoint Security для Linux»	
САНЗ	Средство анализа защищенности	Программный комплекс «Средство анализа защищенности «Сканер-ВС»	
МЭ	Межсетевой экран	Система защиты информации от несанкционированного доступа «Dallas Lock 8.0-К» (модуль «Межсетевой экран»)	
		Программно-аппаратный комплекс «ViPNet Coordinator HW 4»	
		Программный комплекс ViPNet EndPoint Protection	
СКЗИ	Средство криптографической защиты информации	Программный комплекс ViPNet Client 4	
		Программно-аппаратный комплекс «ViPNet Coordinator HW 4»	
Токен	машинный носитель аутентификационной информации	Программно-аппаратный комплекс аутентификации и хранения информации «Рутокен»	

Приложение № 3

ФОРМА

Министру труда и
социального развития
Новосибирской области

Заявка
на подключение к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области»

«____» _____ 20___ г.

Прошу предоставить доступ к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (далее – ТИС СПГ) в соответствии с нижеприведенными сведениями.

Сведения об организации				
Полное наименование организации				
Краткое наименование организации				
Должность руководителя организации				
Фамилия, имя, отчество руководителя организации				
Адрес организации (для переписки)				
Контактные данные организации				
ИНН				
Данные о сотрудниках организации, уполномоченных на работу в ТИС СПГ				
№ п/п	Фамилия, имя, отчество (при наличии)	Должность	Контактный телефон	Адрес электронной почты
1				
2				
...				

В [наименование подключаемой организации] требования нормативно-правовых и руководящих документов уполномоченных органов в области защиты информации выполнены и соблюдаются.

Лица, допущенные к обработке информации, ознакомлены с организационно-распорядительной документации по защите информации в информационной системе [наименование подключаемой организации], подключаемой к ТИС СПГ, а также под роспись предупреждены обо всех видах ответственности, связанных с разглашением информации (в том числе персональных данных).

Приложение:

Приложение 1. Заверенная копия лицензии на право пользования ПО ViPNet Client, наименование сетевого узла ViPNet, номер сети, копию заключения о допуске пользователя СКЗИ к самостоятельной работе.

Приложение 2. Копии документов по результатам проведения мероприятий по защите информации, включая:

– технический паспорт или иной документ, содержащий сведения о составе и размещении технических средств, входящих в состав ИС, подключаемой к ГИС;

– протокол настройки или иной документ, описывающий произведенные настройки средств защиты информации;

– отчет по результатам проведения анализа защищенности (отчет по сканированию)/протокол/акт по результатам проведения анализа защищенности;

– программа и методики аттестационных испытаний;

– протоколы аттестационных испытаний;

– заключение по результатам аттестационных испытаний;

– аттестат соответствия требованиям по защите информации.

<Должность руководителя организации> _____ _____

(подпись) (инициалы, фамилия)

Приложение № 4

ФОРМА

Министру труда и
социального развития
Новосибирской области

Заявка
на актуализацию учетных данных пользователей государственной информационной системы Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области»

«____» _____ 20___ г.

Прошу актуализировать сведения о пользователях *<Наименование информационной системы>* *<Наименование организации-заявителя>*, подключаемой к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (далее – ТИС СПГ) в соответствии с нижеприведенными сведениями.

Сведения об организации	
Полное наименование организации	
Краткое наименование организации	
Должность руководителя организации	
Фамилия, имя, отчество руководителя организации	
Адрес организации (для переписки)	
Контактные данные организации	
ИНН	

Данные о пользователях ТИС СПГ					
№ п/п	Фамилия, имя, отчество (при наличии)	Должность	Контактный телефон	Адрес электронной почты	Примечание
1					*<Сведения, подлежащие актуализации>*
2					
...					

<Должность руководителя организации> _____ _____
(подпись) (инициалы, фамилия)

Приложение № 5

СОГЛАШЕНИЕ О ВЗАИМОДЕЙСТВИИ

при организации работы в государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области»

№_____

г. Новосибирск **«____» _____20___ г.**

Министерство труда и социального развития Новосибирской области» (далее – Минтруда и соцразвития НСО) в лице _____, действующего на основании _____, с одной стороны, и _____ (далее – Поставщик социальных услуг) в лице _____, действующего на основании _____, с другой стороны, совместно именуемые «Стороны», заключили настоящее соглашение о нижеследующем.

1. Предмет соглашения

1.1. Стороны договорились о взаимодействии при работе в едином информационно-коммуникационном пространстве для централизованного ведения данных в государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области» (далее – ТИС СПГ).

2. Обязанности Сторон

2.1. Минтруда и соцразвития НСО:

– обеспечивает создание и ввод в эксплуатацию ТИС СПГ;

– определяет организационные и организационно-технические меры защиты ТИС СПГ;

– обеспечивает бесперебойное функционирование ТИС СПГ;

– производит отключение соответствующей информационной системы от информационных ресурсов ТИС СПГ при выявлении нарушений требований по защите информации с уведомлением организации, ответственной за эксплуатацию отключаемой информационной системы;

– производит повторное подключение информационной системы к информационным ресурсам ТИС СПГ после документального подтверждения устранения нарушений по защите информации.

2.2. Поставщик социальных услуг:

– обеспечивает работоспособность автоматизированных рабочих мест для работы в ТИС СПГ;

– обеспечивает работоспособность программно-технических средств и телекоммуникационного оборудования локально-вычислительных сетей, необходимых для нормального функционирования автоматизированных рабочих мест для работы в ТИС СПГ;

– обеспечивает защиту автоматизированных рабочих мест от вредоносного кода, обнаружение компьютерных вторжений, направленных на использование уязвимостей системного и прикладного программного обеспечения, сетевых протоколов, программно-технических средств, телекоммуникационного оборудования и рабочих станций локально-вычислительных сетей _____;

– несет ответственность за выполнение установленных условий функционирования

информационной системы (далее – ИС), подключаемой к ТИС СПГ, технологии обработки персональных данных и требований по обеспечению их безопасности, а также выполнение требований защиты информации иных сведений ограниченного доступа;

– обеспечивает поддержку соответствия системы защиты ИС, подключаемой к ТИС СПГ, аттестату соответствия требованиям по защите информации в рамках реализации мероприятий по защите информации;

– обеспечивает предоставление в Минтруда и соцразвития НСО скан-копии действующего аттестата соответствия информационной системы, подключенной к информационным ресурсам ТИС СПГ, при повторной оценке эффективности реализованных в рамках системы защиты информации мер по обеспечению безопасности информации, в том числе персональных данных, или аттестации информационной системы, подключенной к информационным ресурсам серверного сегмента ТИС СПГ;

– обеспечивает соблюдение Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» при работе с ТИС СПГ;

– обеспечивает внесение в ТИС СПГ информации о социальных услугах, предоставляемых получателям.

2.3. Стороны обязуются соблюдать требования Регламента подключения к государственной информационной системе Новосибирской области «Территориальная информационная система «Социальный портрет гражданина и типизированное хранилище данных Новосибирской области».

2.4. Стороны обязуются сохранять конфиденциальность обрабатываемой в ТИС СПГ информации.

3. Ответственность Сторон

3.1. Стороны несут ответственность за выполнение настоящего соглашения в соответствии с законодательством Российской Федерации.

4. Прочие условия

4.1. Соглашение составлено в двух экземплярах, имеющих равную юридическую силу.

4.2. Изменения и дополнения в настоящее соглашение вносятся по согласованию Сторон.

4.3. Срок соглашения составляет один год.

4.4. Соглашение не порождает взаимных финансовых обязательств Сторон.

5. Реквизиты и подписи Сторон

Наименование организации	**Министерство труда и социального развития Новосибирской области**
адрес:	адрес:
ИНН	ИНН
Должность	*Должность*
_____ И.О. Фамилия	_____И.О. Фамилия
м.п.	м.п.